

Appl. No. 10/003,776
Amdt. Dated July 28, 2005
Reply to Office action of April 29, 2005
Attorney Docket No. P14206US1
EUS/J/P/05-3170

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of sending encrypted streamed data over an IP network from a first node to a second node, the method comprising:
using Internet Key Exchange (IKE) Phase 1 negotiation to establish an IKE security association (SA) between the first and second nodes;
entering IKE Phase 2 to negotiate an IPsec SA for each transmission direction;
passing the IPsec SA data to streamed data applications associated with the streamed data, ~~using the IKE SA to establish an IPsec SA between the first and second nodes;~~
encrypting the streamed data at the first node with a cipher using a shared secret forming part of said IPsec SA;
constructing IP datagrams containing ~~in their payload segments of the encrypted~~ streamed data, the datagrams not including an IPsec header or headers; and
sending the IP datagrams from the first node to the second node.
2. (Original) A method according to claim 1, wherein said streamed data is VoIP data or videoconferencing data.
3. (Currently Amended) A method according to claim 1, wherein said ~~peer~~ first and second nodes are end points for the data.
4. (Currently Amended) A method according to claim 1, wherein said ~~peer~~ first and second nodes tunnel data between respective end points.

Appl. No. 10/003,776
Amdt. Dated July 28, 2005
Reply to Office action of April 29, 2005
Attorney Docket No. P14206US1
EUS/J/P/05-3170

5. (Currently Amended) An apparatus ~~Apparatus~~ for securing sending streamed data over an IP network ~~to a peer~~ from a first node to a second node, the apparatus comprising:

processing means and memory containing software instructions for implementing IPSec protocols;

an application for delivering streamed data;

~~means for employing components of said processing means and memory containing software instructions for~~ using Internet Key Exchange (IKE) Phase 1 negotiation to establish an IKE security association (SA) between the first and second nodes;

means for entering IKE Phase 2 negotiation to negotiate an IPSec SA for each transmission direction;

means for passing the IPSec SA data to applications associated with the streamed data;

encrypting means for encrypting the streamed data at the first node with a cipher using a shared secret forming part of said IPSec SA;

means for constructing IP datagrams containing the encrypted streamed data, the datagrams not including an IPSec header or headers; and

transmission means for sending the IP datagrams from the first node to the second node.

~~means for using the IKE SA to establish an IPSec SA between the first and second nodes, the IKE SA comprising a shared secret;~~

~~means for encrypting the streamed data with a cipher using the shared secret;~~

~~means for constructing IP datagrams containing in their payload segments of the encrypted streamed data, the datagrams not including an IPSec header or headers; and~~

~~transmission means for sending the IP datagrams from the first node to the second node.~~

Appl. No. 10/003,776
Amdt. Dated July 28, 2005
Reply to Office action of April 29, 2005
Attorney Docket No. P14206US1
EUS/J/P/05-3170

6. (Original) Apparatus according to claim 5, the apparatus being an end user terminal such as a telephone, communicator, PDA or palmtop computer, or a personal computer (PC).

7. (Currently Amended) Apparatus according to claim 6, the apparatus being a firewall or gateway coupled to the first node ~~an end-point~~ which is the source of the streamed data.